Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi (ASEAD)
Eurasian Journal of Social and Economic Research (EJSER)
ISSN:2148-9963 **www.asead.com**

DOLANDIRICILIK GİRİŞİMLERİ VE DOLANDIRICILIKTAN KORUNMA YÖNTEMLERİ

Muhammet TUNAY[1]

ÖZET

Bilişim teknolojilerinde yaşanan hızlı gelişimler ve bilişim araçlarının yaygın şekilde kullanımıyla birlikte elektronik ticaret ve elektronik/dijital bankacılık hizmetlerinde de ciddi iyileşmeler olmuş olup, geleneksel iş yapma tarzları ve iş ilişkileri de değişime uğrayarak yeni tarz iş ilişkileri de değişime uğrayarak yeni tarz iş ilişkileri yaygınlık göstermeye başlamıştır. Bilhassa da bankacılık sektöründe iletişim ve bilgi teknolojilerine dayanan hizmetlerde ciddi gelişmeler ortaya çıkmıştır. Bankacılık ürün ve hizmetlerindeki gelişmeler, şube kanallarıyla beraber alternatif dağıtım kanalları üzerinden sunulmaya başlanmış olup, mekan ve zamandan bağımsız olarak erişime açık olan söz konusu hizmetler müşteriler tarafından büyük ölçüde kabul görmüştür. Dijital ortamlar içinde sunulmuş olan hizmet ve ürünlerin güvenli olarak sunulması, yeni kanallar üzerinden sunulan hizmetlerin yaygınlaşması açısından büyük önem arz etmektedir. İnternet bankacılığı dünyada, ilk olarak 1980'li yıllarda kullanılmaya başlanmıştır. İlk internet bankacığı 1995 senesinde Amerikan "Presidential Savings Bank"ın müşterilerin işlemlerini ve hesap bakiyesini internet üzerinden göstermesi şeklinde uygulamaya alınmıştır. İnternet bankacılığının yaygın olarak kullanılmaya başlanması faaliyetleri 1990'lı yılların sonlarına doğru başlamıştır. Türkiye'de ise ilk internet bankacılığı hizmeti 1997 yılında başlayıp, ürün çeşitliliğiyle beraber hızla yaygınlaşmaya başlamıştır.

Kişisel bilgisayarların 1990'lı yıllarla beraber yaygınlık göstermesiyle hayatımıza giren internet hizmeti yapıları gereği, gerekli güvenlik önlemlerinin alınmamış olduğu durumlarda bazı olası risk faktörlerini bünyelerinde barındırdığı da görünmektedir. İnternet bankacılığını kullanmakta olan müşteriler mevcut risk durumlarında, kendilerini güvende hissetmek adına farklı kişisel önlemler almaya yönelmişlerdir. Bu önlemleri alma bağlamında yeteri kadar bilgiye sahip olmayan müşteriler de, güvenlik taleplerini hizmet sağlayıcılarına iletmişler ve kurumlar, özellikle internet bankacılığı hizmet sağlayıcısı olan bankalar bu konuda ciddi önlemler almaya başlamışlardır.

Anahtar Kelimeler: Dolandırıcılık, Dolandırıcılıktan Korunma Yöntemleri, Dolandırıcılık Bilişim Teknolojileri

[1] Türkiye Halk Bankası A.Ş., Türkiye, ORCID ID: 0000-0001-7092-4696, muhammet.tunay@halkbank.com.tr
Araştırma Makalesi/Research Article, Geliş Tarihi/Received: 24/03/2024–Kabul Tarihi/Accepted: 24/04/2024

FRAUD ATTEMPTS AND FRAUD PROTECTİON METHODS

Muhammet TUNAY

ABSTRACT

With the rapid developments in information technologies and the widespread use of information tools, there have been serious improvements in electronic commerce and electronic/digital banking services, and traditional business styles and business relations have also changed and new style business relations have also begun to become widespread. Especially in the banking sector, serious developments have emerged in services based on communication and information technologies. Developments in banking products and services have begun to be offered through alternative distribution channels as well as branch channels, and these services, which can be accessed regardless of location and time, have been widely accepted by customers. Secure delivery of services and products offered in digital environments is of great importance for the expansion of services offered through new channels. Internet banking was first used in the world in the 1980s. The first internet banking was implemented in 1995, when the American "Presidential Savings Bank" showed customers' transactions and account balances over the internet. The widespread use of internet banking started in the late 1990s. The first internet banking service in Turkey started in 1997 and started to spread rapidly with its product diversity.

Internet services, which entered our lives with the widespread use of personal computers in the 1990s, appear to contain some possible risk factors in cases where the necessary security measures are not taken, due to their nature. Customers using internet banking have tended to take different personal precautions to feel safe in current risk situations. Customers who do not have sufficient information about taking these precautions have conveyed their security requests to their service providers, and institutions, especially banks that are internet banking service providers, have begun to take serious measures in this regard.

Keywords: Fraud, Fraud Protection Methods , Fraud İnformation Technologies

GİRİŞ

Dolandırıcı kelimesi Türk Dil Kurumu sözlüğünde ‘’birisini aldatarak para veya malını alan kimse ‘’ olarak tanımlanır. Dolandırıcılık eylemlerine Dünyanın her yerinde rastlamak mümkündür. Günümüzde teknoloji kullanımının ve uzaktan işlemlerin daha da yaygınlaşmasıyla dolandırıcılık eylemleri teknolojik yöntemlerin kullanıldığı daha karmaşık bir yapıya bürünmüştür.

İletişim sektörünün gelişimi ile birlikte; bireyler arasında davranış, paylaşım ve bilginin gelişimi durumu, beraberinde iletişim ve bilişim konusunda da farklı sıkıntıları beraberinde getirmiştir. (Çolaklar, Gültekin, Şeşen, N. 2023, s.1-12)

Dolandırıcıların veya dolandırıcılık amacıyla kurulan çetelerin hedeflerinde şahıslarla beraber zaman zaman kurumlar da yer alabilmektedir.

Son dönemlere bakıldığında, dijital kanalların artmasıyla beraber çeşitli farklılıklarda dolandırıcılık eylemlerinin de yaşandığı görülmüştür. Ayrıca ciddi artış gösteren dolandırıcılık eylemleri hakkında farkındalıkların oluşması ve alınacak olan güvenlik önlemlerine dair kamuoyuna bilgi verilme durumlarından kaynaklı pek çok teknik/akademik çalışma yapılmıştır.

Dijital platformlarında etkisiyle beraber, sosyal mühendislik temelli dolandırıcılıklar, ATM dolandırıcılıkları, zararlı yazılım kaynaklı dolandırıcılıklar dahil Dijital Bankacılık Kanallarında karşılaşılan çok sayıda dolandırıcılık türü bulunmaktadır. Bunlara ek olarak, kimlik belgeleri, sahte vekaletname, sahte talimat gibi bilhassa banka çalışanlarının da karıştığı bilgi ve belge sahteciliği konularını da çok sıklıkla görülmektedir.

Raporlara bakıldığında, işletmelerin ortalama %33'lük kısmının yıldan yıla artış gösteren dolandırıcılık saldırısı yaşadığı tahmin edilmektedir. Zimmete para geçirme ve varlıkların kötüye kullanılma durumları benzeri tespit edilmeyen dahili sorunlar, işletmeleri daha fazla dolandırıcılık amaçlı finansal raporlamaya açık bırakarak, devlete ödenen gelir vergisinin miktarını azalttığı gibi, kurumun da gelir kaybını artıracaktır.

Dolandırıcılığın önlenmesi, dolandırıcılığın yapılmasından daha önce kurumu koruyabildiği için, her kurumun bir stratejik planı olmalıdır. Adli muhasebe hizmetleri bu durumları önleyebilir ve mali suçları ortaya çıkarabilir. Çalınan paranın nereye gittiği ve onu nasıl geri alacağı ile ilgili anlamlandırmaya da yardımcı olabilir.

1. KAVRAMSAL ÇERÇEVE

1.1 İş Dolandırıcılığı Türleri

A-)İş sahtekarlığı birçok biçimde meydana gelir ancak üç kategoriye ayrılabilir: varlıkların kötüye kullanılması, yolsuzluk ve mali tablo sahtekarlığı bunlardan bazılarıdır. Varlıkların zimmete geçirilmesi, en az maliyetli olmasına rağmen, incelenen tüm dolandırıcılık vakalarının %90'ını oluşturmaktadır. Bunlar, bir çalışanın kuruluşunun kaynaklarını çaldığı veya sömürdüğü planlardır. Varlıkların kötüye kullanılmasına örnekler, kaydedilmeden önce veya sonra nakit çalmak, yanlış gider geri ödeme iddialarında bulunmak ve/veya kuruluşun nakit olmayan varlıklarını almaktır. (Özcan, N. 2012, s.74).

B-) Mali tablo sahtekarlığı, vakaların yüzde beşinden daha azını oluştursa da ciddi kayıplar doğurduğu görülmektedir. Bunlar, şirketin finansal raporlarındaki bilgilerin atlanmasını veya kasıtlı olarak yanlış bildirilmesini içeren planlardır. Bu, hayali gelirler, gizli yükümlülükler veya şişirilmiş varlıklar şeklinde olabilmektedir. (Özcan, N. 2012, s.74).

C-) Yolsuzluk planları, çalışanlar işverene karşı görevlerini ihlal ederken ticari işlemlerdeki etkilerini kendi çıkarları için kullandıklarında ortaya çıkar. Yolsuzluk örnekleri rüşvet, haraç ve çıkar çatışmasıdır. (Özcan, N. 2012, s.74).

D-) Elektronik bankacılık kanallarında karşılaşılan dolandırıcılık türlerini 6 başlık altında inceleyebiliriz. (URL 1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.1- Zararlı yazılım kaynaklı dolandırıcılıklar; Zararlı yazılımlar, programlanabilen herhangi bir ağa, aygıt veya hizmetlere zarar vermek amacıyla ya da bunlardan yararlanmak için tasarlanmış tüm kötü niyetli yazılımlar için kullanılan kapsamı geniş bir terimdir. Siber suçlular genelde bunları, maddi getiri elde etmek amacıyla mağdurlardan veriler elde edip baskı yapmak amacıyla kullanmaktadır. Ele geçirilen veriler kişisel verilerden mali verilere, e-postalara, sağlık kayıtlarına, parola ve şifrelere kadar değişebilir. (URL 1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Bankaların müşterileri gelişen ve değişen teknolojilerle beraber ortaya çıkmış zararlı yazılımların en büyük hedef ve kurbanlarındandır. Zararlı yazılımları geliştiren şahıslarca bu zararlı kodlar karanlık internet ağı olarak isimlendirilen yasa dışı elektronik ortamlarda satılmakta ve bunları satın alan kişiler tarafından dağıtılabilmektedir. (URL 1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Ülkemizde bankacılık sektöründe karşımıza çıkan zararlı yazılımlardan ilk olarak İnternet Bankacılığı kullanan müşteriler etkilenmiştir. Bunlara yönelik BDDK tarafından 2008 senesinde yürürlüğe alınan Tebliğ'le bankaların sistemleri üzerinde gerekli önlemleri almaları hedeflenmiştir. Sürekli değişen ve gelişen yöntemlere sektörel bazda önlemler alınabilmesi nedeniyle 2020 senesinde yeni yönetmelik yürürlüğe alınmıştır. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Zararlı Yazılım Türleri: İnternet/Mobil bilgi hırsızlığı çeteleri çeşitli yollarla müşterilere ait özel ve kişisel bilgileri ele geçirmektedirler. Bu yöntemlerin en sık kullanılanları aşağıda sıralanmıştır.(URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.1.1- Truva yazılımları (Trojan) : Truva (Trojan) yazılımlarının adı Truva Atı'ndan gelmektedir. Bir bilgisayarda bulunan programa bağlanıp gizlenen, zarar verirken ise, sistemin normal çalışmasına izin verir gibi görünen virüse '' Truva Atı'' denir. Truva atı genelde, bulaştığı bilgisayarda kullanılmakta olan, kullanıcı adı, parola gibi özel ve kişisel bilgilere sahip olmak amacıyla kullanılır.

Tespiti oldukça güç olan Truva atı, genelde sistemlere e-posta yolu ile bulaşmaktadırlar. Bununla beraber cd, dvd , e-mail ekinde gönderilen (.doc , .jpg , .txt , .gif , .xls. vb.) dosyalara, bilgisayar oyunlarında bulunan ''.exe'' uzantıdaki uygulama dosyası gibi yerlere gizlenebilirler. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.1.2 – Ekran ve Tuş Kaydediciler (Screenlogger ve Keylogger): Tuş kaydedici, bilgisayarlarda, klavye tuşlamalarını, vuruşlarını anlık olarak kopyalayan, bu kopyalamaları kaydedip e-mail vasıtasıyla zararlı yazılımcının ele geçirmesine imkan veren programlardır. Bu program klavyeyle yazılabilen tüm verileri kaydetme yeteneğine sahiptir.

Ele geçirilen veriler sistemde ‘’.txt.’’ uzantıdaki metin dosyası olarak tutulur. Yapısı gereği kurbanın her türdeki parola ve kişisel yazışmasını ele geçirmek amacıyla kullanılabilir.

Ekran kaydedicilerse, ekran görüntülerini anlık olarak kopyalayıp, kopyalanan verileri e-mail yoluyla korsanların eline geçmesini sağlayan programlardır. Alınan ekran görüntüleri sayesinde, o sırada ekranlarda yapılanlar ya da parolaların hangi kısma yazıldığı kolayca görünebilir. Ekran ve Tuş kaydediciler dolandırıcılık işlemlerinde birbirini tamamlayan 2 bileşen gibi çalışırlar. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.1.3 – Pop-Up Ekranlar: Bir arıza bildirimi, erişim ve yetki sorunu, yardım, yenileme teklifi, geliştirme vb. içeriklerle kullanıcı karşısına çıkan ekrana, kullanıcı adı ve parola girişi talep edilerek erişim yetkisi çalınır. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Bu dolandırıcılık tipinde, kullanıcıya bir pop-up uyarı mesajı ile cihazında tespit edilmiş bir eksiklik ve aksaklıktan kaynaklı bazı programların çalışmayacağını gösterir bir uyarı mesajı çıkarır. Aynı mesajda kullanıcıya ‘’hemen yükleyin’’ gibi ücretsiz bir yardımcı program teklifinde bulunur. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.1.4 – Spam E-Postalar: Genellikle istenmeyen ve gereksiz mesaj olarak da isimlendirilen bu e-mailler, içinde bulunan zararlı yazılım barındırabildiği gibi, zararlı yazılımlara sebep olan sayfalara da yönlendirmektedirler. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.1.5 – Teknolojik Donanımlar: Art niyetli şahıslar, kurbanlara ait özel ve kişisel bilgileri teknolojik imkanlarla (dinleme, casusluk vb.) ele geçirir. Özellikle resmi ve özel kurumda çalışan hizmet ve temizlik personelleri ya da kurbanlara yakın olan güvenlerini kazanabilecek art niyetli şahıslar, klavye ve mouse kablolarının ucuna yerleştireceği bir kopyalama aygıtı (donanımsal keylogger) ile tüm gün personelin ekranını ya da yazdıklarını kopyalayıp, daha sonra yapılacak temizlik gününde ise veriler kurum dışına sızdırılmış olacaktır. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Zararlı yazılımdaki hedef bireyin kendine has bankacılık işlemlerinde kullandığı kişisel veriler ve kendince belirlenen parolalardır. Bu verileri ele geçiren dolandırıcının aynı zamanda müşteriye ait telefona gönderilen tek kullanımlık OTP-SMS bilgilerini de ele geçirmesi gerekmektedir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Ocak 2021 itibarıyla İnternet Bankacılığı kullanımları Mobil Uygulama onayına tabi olmuştur. Yeni Yönetmelikle yalnız mobil uygulamasını aktif etmemiş olan müşteriler OTP-SMS ile işlemlere devam edebilecektir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.2 – Sosyal Mühendislik Temelli Dolandırıcılıklar: Bütün sosyal mühendislik yöntemleri, şahısların davranış ve hareketlerinde bulunan önyargılar temeline kurgulanmaktadır. Bu önyargılar insanlara ait ‘’sistem açığı’’ olarak da tanımlanabilmektedir.

Bu yöntemleri kullanan kişiler, insan davranışlarındaki önyargıyı harekete geçiren metotları büyük bir ustalık ile kullanan kişilerdir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Bu yöntemlerini kullanan dolandırıcıların amacı, kurum ve kişilere ait bilgi ve verileri (çalışma koşullarını, fiziki, sistemsel çevreleri, iş akışları, kullanıcı kod ve parolaları, güvenlik organizasyonu, organizasyon şemaları vb. materyalleri) teknolojiyi kullanmadan ya da teknolojik imkanlarla haksız çıkarlar elde etmektir.

Sosyal mühendislikte temel kandırmaya yöneliktir. Sosyal mühendislik vakaları karşıdakini yanıltma, kandırma yolu ile verilerin ele geçirildiği an itibariyle başlayarak, elde edilen haksız çıkarların da dahil olmasıyla sürecin tamamını ifade etmektedir.

Aşağıda belirtilen senaryolar, bireylerin karar verme eğilimlerini etkilemek (manipüle etmek) amacıyla en sık kullanılan yöntemlerdendir;

*Otorite korkusu; ‘’savcılıktan telefon ediyoruz’’ terör örgütleriyle bağlantılı olduğunuz tespit edilmiştir. ‘’tehdit mesajları göndermişsiniz…’’

*Yardım etme arzusu; ‘’tabi hemen…’’

*Kazanma arzusu; ‘’ödül ve puan kazandınız’’ mesajları

*Üşengeçlik; ‘’ İşlemleriniz için şubeye gelmenize gerek yok, biz hemen halledelim siz yorulmayın…’’

*Ego, Değer görme duygusu: ‘’ sizin gibi kıymetli biri ile iş yapıyoruz, kişisel numaranızı verebilir misiniz? … ‘’

*Vaadcilik; ‘’Kredi dosya masraflarını , kredi kartı kullanım ücretlerini geri alırız…’’

*Güvenlik korkusu; ‘’ Hesabınızdan bilginiz dışında işlem yapılmıştır işlem iptali için parolanızı paylaşır mısınız? …’’

*Yetersiz bilgi; ‘’Kart ya da hesap numaramı verince ne olacak ki?’’

*Kaybetme endişesi; ‘’Bu kampanya sadece bugüne özel sunulmuştur…’’

D.3 – Çağrı Merkezi (Müşteri Hizmetleri) Dolandırıcılıkları: Bankalar, müşteri hizmetleri (çağrı merkezleri) kanalını şubelere en büyük alternatif kanal olarak, internet ve mobil bankacılık vb. elektronik kanalların yaygınlaşıp gelişmesinden çok daha önceleri kullanmışlardır. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Gelinen zamanda da nakit gerektiren durumlar dışında, hemen hemen bütün bankacılık işlemlerinin yapıldığı bu kanalda müşteriler sesli yanıt sistemi, akıllı yönlendirmelerle olabilecek en kısa sürede hizmet almayı talep ettiği menüye yönlendirilmektedir, işlemlerini bankanın çalışanları vasıtasıyla veya sesli yanıt sistemiyle kendisi bizzat yapabilmektedir.

Ses tanıma vb. biyometrik doğrulama yönteminin kullanıldığı çağrı merkezleri kanallarında, mobil ve internet bankacılığı kanallarına ait parolaların kullanımları müşterilerin deneyimleri açısından bankalar tarafından en çok tercih edilen yöntemlerdir. Bu kanallardan yapılan doğrulama yöntemi ve işlem çeşitliliğinin diğer kanallarla ortak olması, değişik yöntemler ile ele geçirilen müşterilerin bilgi ve verileri üzerinden dolandırıcılık eylemlerinin gerçekleşmesini de beraberinde getirmektedir.

Çağrı merkezi dolandırıcılıkları, müşteri verilerinin (kart, kimlik, sim kart, internet, mobil bankacılık, vb.) ele geçirilerek üçüncü kişilerce müşteri hizmetlerinin aranması ile asıl müşteri adına işlem yapılmasıdır.

Bu dolandırıcılık eylemi zaman geçtikçe değişiklik gösterse bile günümüzde hala yeni teknolojileri kullanan art niyetli çeteler Çağrı Merkezi aracılığıyla müşterilerin hesaplarına erişebilmektedirler.

D.4 – Sim Kart Kopyalama: Müşterinin adına düzenlenen sahte kimlik ile, telefonun çalındığı ya da kaybolduğunu beyan ederek GSM operatörlerinin bayilerinden yeni bir SİM kart alarak müşterilerin banka hesap bilgilerinin ele geçirilmeye çalışıldığı dolandırıcılık şeklidir. Bu yöntem kullanıldığında SMS ile gönderilen tek kullanımlık şifre ve geçici statik şifreler doğrudan dolandırıcının eline geçmektedir.(URL1:https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.5 – ATM Dolandırıcılıkları: Banka müşterisinin şubeye gelmeden para çekip, yatırabilmesi amacıyla geliştirilmiş ATM kanalı, gelinen zamanda kredi başvurusu, para transferi, bilgi güncelleme vb. başka temel bankacılık işlemleri için de hizmet sunan bir alternatif dağıtım kanalı haline gelmiştir. Müşterinin ihtiyaç duyduğu anda kısa zaman içinde temel bankacılık ihtiyaçlarını karşılayabilmesi adına şube lokallerinden farklı konumlara ATM kurulumları yapılabilmektedir. Dolandırıcılarca ATM kanalına özel ve farklı yöntemlerle müdahalede bulunularak müşteri hesap ve kart bilgilerinin ele geçirilmesi hedeflenmektedir.(URL1:https://www.tbb.org.tr/tr(Erişim Tarihi: 05.01.2022)

Bu dolandırıcılıklar, yetkisi bulunmayan donanım ve yazılımlarla ATM'nin manipüle edilmesiyle müşterilerin bilgisinin, müşterilerin kartlarının ya da ATM'ye ait sistemin ele geçirilmesi olarak özetlenebilir.

D.5.1 – ATM Kart Kopyalama: Kopyalama aygıtları vasıtasıyla dolandırıcılarca ATM'nin içine ya da üstüne yerleştirilerek kart bilgilerinin ve manyetik verilerin geçirilmesidir. Kullanılan bu yöntemde kartın parolasının ele geçirilmesi ATM'nin klavyesinin üzerine yerleştirilmiş sahte bir klavye düzeneği ile ya da ATM'nin üzerine yerleştirilen klavyeye odaklı bir gizli kamerayla yapılabilmektedir.(URL1:https://www.tbb.org.tr/tr(Erişim Tarihi: 05.01.2022)

D.5.2 – ATM Para Sıkıştırma: Para çekme bölümünün kapak kısmına benzeyen sahte bir kapağın üzerine sürülmüş yapıştırıcı veya dışarıdan para çekme bölümüne müdahale ile eklenen bir aygıt vasıtasıyla ATM'nin içinden çıkan paraların, dolandırıcılarca daha sonra alınmasıdır.

Hesaptan çekilen para, çıkış bölümü kapağı ile sonradan eklenen sahte kapağın arasında sıkışmış ya da gizlenmiş durumdadır. Müşteri ATM'den parayı çekmiş ancak para çekme bölümü açıldığında hesaptan düşen tutar para çekme haznesi içinde bulunmamaktadır. Müşteri ATM'nin yanından uzaklaştıktan sonra dolandırıcılar sahte kapakta bulunan yapıştırıcıyla tutulan paralara el koyar. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.5.3 – ATM Kart Sıkıştırma: ATM'ye ait kart okuyucusu kısmına dolandırıcı tarafından yabancı cisimler yerleştirilmesi ve kartın üçüncü kişiler tarafından ele geçirilmesidir. Kullanılan bu yöntemde dolandırıcılar genelde sıkışan kartın sahibi ile temas içerisindedir. Müşteriyi makinede sorun olduğuna inandırarak müşteriye yardım etmeye çalışıyor gibi görünüp müşteriyi kartın parolasını tuşlamaya ikna ederler, bu sırada parolayı müşteriden doğrudan ya da dolaylı bir şekilde (omuz sörfü yöntemi gibi) öğrenirler. Dolandırıcılarca makinede bir sorun olduğuna ikna olan müşteriyse makineden uzaklaşır ya da ayrılmaya zorlanır. Müşteri ayrıldıktan sonra sıkışan kart dolandırıcılar tarafından cımbız ya da cımbıza benzer aygıtlar ile ATM'den alınarak parolası ile kullanılır.(URL1:https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.5.4 – Jackpotting (BlackBox): Jackpotting, dolandırıcılar tarafından yetkisiz donanım ve yazılımın bir arada kullanılması ile ATM sisteminin ele geçirilmesi ve para çıkış fonksiyonunun manipüle edilmesidir. Bu yöntemde dolandırıcılar tarafından bir ağ üzerinden veya doğrudan ATM bilgisayarına bir donanım aracılığıyla erişilip ATM'nin mevcut yazılımı manipüle edilir. Bu dolandırıcılık türünün diğerlerinden farkı müşteri bilgisi, müşteri kartı/şifresi gibi bilgilere ihtiyaç duyulmamasıdır. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

D.6 – POS (Point Of Sale) Dolandırıcılıkları: Klasikleşen bir ödeme yöntemi olarak kullanılmakta olan POS sistemleri, yaygın ve yoğun kullanımları sebebiyle dolandırıcılarca hedeflenmiş ciddi bir kanaldır. POS makineleri kart kopyalamalarında kullanıldığı gibi, sanal ortamlarda ele geçirilen kart bilgileriyle işlem yapma amacıyla da dolandırıcılarca kullanılabilmektedir. Ayrıca ödeme aracılığına hizmet etmesi beklenen POS cihazının usulsüz şekilde amaç dışı kullanıldığı da görülebilmektedir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

E-) Bilgi ve Belge Sahteciliği; Art niyetli kişilerce düzenlenmiş sahte veri, bilgi ve belgelerle (sahte hesap cüzdanı, kimlik, talimat vb.) banka ve diğer kurumlara başvuruda bulunularak, bazı işlemler yapılabilmektedir. Teknolojik gelişmeler ve bu gelişmelerin bankacılık sistemindeki kullanımının yaygınlaşmasıyla beraber bankaların sistemlerinde çok sayıda başvuru kontrol mekanizmaları kurulmuş olmasına karşın art niyetli kişilerin de bu gelişen ve değişen teknolojiye ayak uydurarak kullanmış oldukları teknikleri geliştirdikleri görülmektedir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

E.1 – Sahte Kimlikle Yapılan Dolandırıcılıklar: Ele geçirilen ya da kaybolan kimlik belgesi ile oluşturulmuş sahte kimliklerle bankalarda en çok gerçekleştirilen kötü amaçlı işlemler aşağıda belirtilmiştir; (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

* Kredi kartı, kredi, ek hesap/Kredili Mevduat Hesabı(KMH)/Açık hesap ve limit artırım başvurusunda bulunulması

* Şirket kurarak Bankadan kredi, çek koçanı(karnesi) talep edilmesi

* Borç taahhüdüne girilerek kefil olunması

* Mobil ve internet bankacılığı başvurusunda bulunulması

* Cep telefonu ekleme, silme, güncelleme işlemlerinin yapılması

* Nakit çekim ve Para aktarımı(transferi) gibi parasal işlemlerin yapılması

E.2 – Sahte Talimatlarla Yapılan Dolandırıcılıklar: Gelinen zamanda bankacılık hizmetlerinin uzaktan yapılması büyük önem kazanmakla beraber, müşterilerin mobil ve internet bankacılığı gibi kanallardan yapamayacakları tutardaki işlemler için ise uzaktan talimat vererek işlem yapabilmeleri sağlanmaktadır. Bu gibi talimatlar müşterilere ait bankalardaki kayıtlı faks veya e-postaları üzerinden alınmaktadır. Çoğunlukla ticari firmalar ve şahıs işletmelerinin ticari faaliyetlerine ait ödemeler talimatla yapılmaktadır. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Sahte talimatla gerçekleştirilen dolandırıcılıklar, müşteri e-postasının taklit edilmesi ya da ele geçirilmesiyle şube personeline gönderilen sahte talimat veya müşterinin adına banka şubesine faks yoluyla sahte talimat gönderilmesiyle müşterinin hesaplarından para transferi yaptırılmak istenmesidir. Bankaca gerekli sistemsel kontroller yapılsa bile e-mail hesaplarının güvenliği gibi müşterilerce de dikkat edilmesi gereken hususlar bulunmaktadır.

E.3 – Şirket E-postasının Ele Geçirilmesi ile Yapılan Dolandırıcılıklar: Banka müşterisinin, ticari faaliyet içinde bulunduğu firma ya da şahısların e-posta adresleri taklit edilebilmekte ya da ele geçirilebilmektedir. Taklit edilen/Ele geçirilen e-mail adresinden dolandırıcıya ait yeni bir IBAN/hesap/ numarası gönderilerek para transferinin bundan sonra bu IBAN'a/hesaba gönderilmesi talep edilmektedir. Banka müşterisiyse ticari faaliyette bulunduğu firma ya da şahsın bu gönderisine istinaden Bankaya verdiği talimatlardaki alıcı hesap numaralarını değiştirmek suretiyle para transferini gerçekleştirir. Gerçek alıcısına yapılacak ödeme yapılmadığı için belirli bir müddet sonra dolandırıcılık vakası fark edilir. Bu tür dolandırıcılık vakalarının tespitinde ve önlenmesinde firmaların kendisine ait yazışmalarında kullanılan e-mail adreslerinin güvenliğini sağlaması büyük önem arz etmektedir.(URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

E.4 – Şirketin Üst Düzey Yöneticisinin E-postasının Ele Geçirilmesi ile Yapılan Dolandırıcılıklar: Firmanın üst düzey yöneticilerinin (CFO/CEO vb.) elektronik postalarının taklit edilmesi ya da ele geçirilmesiyle firmanın muhasebe/finans çalışanına e-mail yoluyla sahte talimatlar gönderilerek, çalışan personele iletilen bu bilgiler ile para transferi yapılmasını istemesidir.

Bu yöntemde, firmanın üst yöneticisi gibi davranılıp telefon ve diğer iletişim kanalları (anlık mesaj gönderme vb.) üzerinden bankalardan bilgi edinilme ve hatta para transferleri yapılmaya çalışılmaktadır. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

E.5 – Sahte Vekaletname ile Yapılan Dolandırıcılıklar: Vekaletname; müşterinin kendisine ait işlemleri, takip etmesi, yürütmesi, amacı ile tayin edilen vekilin yetki alanını gösteren ve Noter aracılığıyla düzenlenmiş belgelerdir. Bu belgeler aracılığıyla para transferi, para çekme dahil çok sayıda bankacılık işlemleri yapılmaktadır. Bu sebeple, kimlik belgelerinde yapılan sahtecilik girişimlerine benzer bir şekilde; (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

- Tamamıyla sahte bir vekaletname belgesi düzenlenmek suretiyle herhangi bir noter aracılığıyla onaylanmış gibi işlem yapılmaya çalışılabilir,
- Sahte belge ve kimliklerle bankanın müşterisi gibi görünüp gerçek bir noterden gerçek bir vekaletname hazırlatılabilir.

F-) Uzaktan Kimlik Tespiti ve Müşteri Edinimi; Uzaktan kimlik tespiti, müşteri temsilcileri ile kişinin; fiziksel olarak aynı ortamda bulunmasına gerek kalmadan, çevrimiçi olarak görüntülü görüşme yöntemiyle birbiriyle iletişime geçmesidir. Uzaktan kimlik tespiti için müşterinin muhakkak yeni TC Kimlik Kartına ve akıllı cep telefonuna sahip olması gerekmektedir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Uzaktan müşteri olmak istendiğinde, bankaların web sitesi aracılığıyla ya da mobil bankacılık uygulamaları aracılığıyla başvuru formu doldurup başvuruda bulunmaları gerekmektedir. TC Kimlik Kartı ve güvenlik doğrulamaları aracılığıyla şube ve evrağa bağlı kalmadan daha hızlı bir şekilde banka müşterisi olunabilmektedir.

Uzaktan müşteri ediniminde, yüz doğrulama, çipli kimliklerdeki bilgilerin temassız olarak okunması gibi adımlar sürecin daha hızlı ve güvenli oluşmasını sağlamaktadır.

Uzaktan Müşteri Edinim sürecinin yasal dayanağı ve güvelik standartlarının oluşturulması amacıyla BDDK tarafından yapılan çalışmalar sonucunda, Bankalarca Kullanılacak Uzaktan Kimlik Tespiti Yöntemlerine ve Elektronik Ortamda Sözleşme İlişkisinin Kurulmasına İlişkin Yönetmelik 1 Mayıs 2021 tarihinde yürürlüğe girmiştir.

1.2. Dolandırıcılığı Önleme Stratejileri

Büyük ya da küçük bir kuruluş için bir dolandırıcılık önleme planına sahip olmak hayati önem taşır. ACFE 2014 Raporu'nda incelenen dolandırıcılık vakaları, incelenen dolandırıcılık faaliyetlerinin tespit edilmeden önce ortalama 18 ay sürdüğünü ortaya koymuştur. 1,5 yıl boyunca dolandırıcılık faaliyeti sürdüren bir çalışanın, kendi şirketine vereceği zararları tahmin etmek zor olduğu gibi, şirkete çok ciddi yük getirdiği aşikardır. Bunun yanında, farklı prosedürler ve kontroller uygulayarak dolandırıcılık olaylarını en aza indirmenin de teknik yöntemleri bulunmaktadır.

1.3. Dolandırıcılığı Önlemede Temel Faktörler

1.3.1. Çalışanların Tanınması

Suistimal failleri genellikle çalışanın suistimal etme niyetini gösterebilecek davranışsal özellikler gösterirler. Çalışanları gözlemlemek ve dinlemek, potansiyel dolandırıcılık riskini belirlemeye yardımcı olabilmektedir. Yönetimin çalışanlarıyla ilgilenmesi ve onları tanımak için zaman ayırması da önemlidir. Çoğu zaman, bir tutum değişikliği sizi bir riske soktuğu da görülmektedir. Bu, ele alınması gerekli olan iç problemleri de gün yüzüne çıkarmaktadır. Örnek vermek gerekirse de bir çalışan işletme sahibi tarafından takdir edilmediği ya da patronuna öfke duymuş olduğu hissine kapıldıysa, bu onu çalışan sahtekarlığı oluşturmaya yönelttiği de görülmektedir. Çalışanda izlenen herhangi bir tutum değişikliği, o çalışana çok dikkat edilmesine neden olmalıdır. Bu, yalnızca dolandırıcılıktan kaynaklanan bir kaybı en aza indirmekle kalmaz, aynı zamanda kuruluşu daha mutlu çalışanlarla daha iyi, daha verimli bir yer haline getirebilir. Çalışanları dinlemek başka ipuçlarını da ortaya çıkarabilir.

1.3.2. Çalışanları Bilgilendirme / Raporlama Sisteminin Kurulması

Farkındalık tüm çalışanları etkiler. Kuruluş içindeki herkes, dolandırıcılık türleri ve bunlarla ilişkili sonuçlar da dahil olmak üzere, dolandırıcılık riski politikasının farkında olmalıdır. Dolandırıcılık yapmayı planlayanlar, yönetimin izlediğini bilecek ve bu durumdan caydırılacaktır. Dolandırıcılık yapmaya teşvik edilmeyen dürüst çalışanlar da olası dolandırıcılık veya hırsızlık belirtileri konusunda bilgilendirilecektir. Bu çalışanlar, dolandırıcılıkla mücadelede birer varlıktır. (Erdoğan, M. 2021, s.10)

1.3.3. İç Kontrolleri Uygulama

İç kontroller, şirketini varlıklarını korumak, muhasebe kayıtlarının bütünlüğünü sağlamak ve dolandırıcılık ve hırsızlığı caydırmak ve tespit etmek için uygulanan planlar ve/veya programlardır. Görevlerin ayrılığı, hile riskini azaltabilen iç kontrolün önemli bir bileşenidir. Örneğin, bir perakende mağazasında bir yazar kasa çalışanı, bir satış elemanı ve bir yönetici bulunur. Kasa ve çek defteri makbuzları bir çalışan tarafından tutulurken, diğeri depozito fişini hazırlar ve üçüncüsü depozitoyu bankaya getirir. Bu, koleksiyonlardaki tutarsızlıkları ortaya çıkarmaya yardımcı olabilir. Her çalışan diğer çalışan tarafından kontrol edilmelidir.

Dokümantasyon, dolandırıcılığın azaltılmasına yardımcı olabilecek başka bir iç kontroldür. Yukarıdaki örneği incelersek; satış makbuzları ve banka depozitolarının hazırlanması defterlerde belgelenmişse, işletme sahibi makbuzların bankaya yatırıldığını doğrulamak için günlük veya haftalık belgelere bakabilir. Ayrıca, tüm çeklerin, satın alma siparişlerinin ve faturaların ardışık olarak numaralandırıldığından emin olunmalıdır. Gelen tüm çeklerde "yalnızca depozito için" damgası kullanılır, belirli bir doların üzerindeki çeklerde iki imza gerektirir ve imza damgası kullanmaktan kaçınılmalıdır. Ayrıca, fatura düzenini zimmete geçirenler kurarken ve genellikle bir Posta Kutusuna postalanan hayali satıcılara ödeme yaparken yeni satıcılara karşı dikkatli olunmalıdır.

İç kontrol programları, teknolojik ve diğer gelişmelerle etkin ve güncel olduklarından emin olmak için tutarlı bir şekilde izlenmeli ve revize edilmelidir. Bir iç kontrol süreci veya çalışan dolandırıcılığı önleme programı yoksa, bu alanda deneyimli bir profesyoneli işe almakta önem arz etmektedir. Bir uzman, şirketin politikalarını ve prosedürlerini analiz edecek, uygun programları önerecek ve uygulamaya yardımcı olacaktır.

1.3.4. Güvenilir Uzmanlar İşe Alın

Sertifikalı Dolandırıcılık Denetçileri, Yeminli Mali Müşavirler ve Sahtecilik Adli Tıp Sertifikalı CPA'lar da dahil olmak üzere şirketler için çalışan kişilerin çoğu, dolandırıcılık karşıtı politika ve prosedürlerin oluşturulmasında önemli roller oynayabilir. Ancak, bu uzmanların tümü, ihtiyaçlarınız için en iyi hizmeti sağlama konusunda deneyime veya itibara sahip değildir. Banka hesap numaraları gibi hassas şirket bilgilerine erişimi olacak muhasebecileri, dolandırıcılık denetçilerini ve diğer uzman profesyonelleri işe alırken, bu firmaların veya bireylerin kaliteli hizmet ve güvenilirlik üzerine kurulu bir itibara sahip olmalarını sağlamak çok önemlidir. Bu sayede adli analizler, temel finansal danışmanlık hizmetleri ve iç kontrol denetimlerinizden emin olunmalıdır.

1.3.5 İnsanlar Tarafından Alınabilecek Önlenmeler

Bildirimlerle akıllı cihazlara gelen linklerin, kaynağından emin olunmamış SMS(kısa mesaj), sosyal medya reklamları, anlık haberleşme uygulamalarından gelen bildirimler ve e-mail gönderileri açılmamalı ve içerisinde bulunan linkler tıklanmamalıdır.

Kimlik bilgilerinin gizliliği konusunda, bankacılık işlemlerinde kullanılacak kimliklerin güvenliği son derece önemli iken; kimliklerin taranmış görüntülerinin bilgisayarda muhafaza edilmemeli, fotokopileri rastgele yerlerde bulundurulmamalıdır.

Parola/Şifre Bilgilerinin Gizliliği: Bankacılık işlemlerinde kullanılan parola/şifre kişilere özel durumdadır ve gizliliğinin/güvenliğinin sağlanması müşterilerin sorumluluğundadır. Parola/Şifre bilgilerinin kolay tahmin edilemeyecek şekilde (doğum yılı vb.) oluşturulması da büyük önem arz etmektedir.

Ortak kullanım için tahsis edilen ve güvenliğinden de çok emin olunamayan cihazlardan bankacılık kanallarına/uygulamalarına giriş yapılma halleri önerilmemekte olduğu görülmektedir. Dahası kamuya (ortak kullanıma) açık kablosuz ağ bağlantıları üzerinden bankacılık işlemlerinin yapılmamasına özen gösterilmelidir. POS ve ATM gibi ortak kullanıma açık alanlarda yapılan bankacılık işlemlerinde kullanılan parolaların, üçüncü kişiler tarafından görülmeyecek şekilde tuşlanması önemlidir.

Bankalar Tarafından Gönderilen Bildirimler: Ürünlerin güvenliğiyle alakalı hususlar hakkında bankalarca verilen açıklamaların/bilgilerin okunması ve belirlenmiş talimatlara uygun hareket edilmesi güvelik açısından büyük önem arz etmektedir. Güvenlikle alakalı herhangi bir tereddüt olması durumunda derhal bankaya başvurulmalı ve banka bilgilendirilmelidir.

Bankalar tarafından ilan edilen güvenlik duyuruları sürekli takip edilmeli ve bu duyurularda ilan edilen uyarılara dikkat edilmelidir. (Yelken, C. 2019, s 66)

İletişim Bilgilerinin Güncelliği: Bankaların müşterileri namına yapılan işlemler ile ilgili bilgilendirme yaptığı ve şüpheli işlem bildiriminde ulaşmak için kullandığı iletişim adreslerinin (e-posta bilgisi, cep telefonu numarası, ev/iş adresi vb.) banka kayıtlarında sürekli güncel tutulması büyük önem arz etmektedir. Bu adreslerde yapılacak değişiklikler müşteriler tarafından bankaya zamanında bildirilmesi çok önemlidir.

1.3.6. Kurum Kültürü

Olumlu bir çalışma ortamı, çalışanların dolandırıcılığını ve hırsızlığını önleyebilir. Açık bir organizasyon yapısı, yazılı politikalar ve prosedürler ve adil istihdam uygulamaları olmalıdır. Açık kapı politikası, çalışanlara yönetimle açık iletişim hatları sağladığı için harika bir çalışan dolandırıcılık önleme sistemi de sağlayabilir. İşletme sahipleri ve üst düzey yönetim, örnek olarak liderlik etmeli ve pozisyonu ne olursa olsun her çalışanı eylemlerinden sorumlu tutmalıdır.

1.4. Dolandırıcılık Tespit Stratejileri

Önleme stratejilerine ek olarak, tespit yöntemlerine de sahip olmak ve bunları çalışanlara görünür kılmak da gerekmektedir. Etkili olduklarından emin olmak için dolandırıcılık tespit stratejileri sürekli olarak izlemek ve güncellemek önemlidir. Algılama planları genellikle düzenli olarak planlanan iş günü içinde gerçekleşir. Bu planlar, dahili verilerle bağlantı kurmak için harici bilgileri dikkate alır. Dolandırıcılık tespitinin sonuçlarını alanlar önleme kontrollerinizi geliştirmelidir. Her görevden sorumlu kişiler veya ekipler dahil olmak üzere dolandırıcılık tespit stratejilerini de belgelemek önemlidir. Nihai dolandırıcılık tespit planı tamamlandıktan sonra, tüm çalışanlar plan ve bunun nasıl uygulanacağı konusunda bilgilendirilmelidir. Bunu çalışanlara iletmek başlı başına bir önleme yöntemidir. Şirketin izlediğini ve disiplin cezası alacağını bilmek, çalışanların dolandırıcılık yapma planlarını engelleyebilir. (Özmen, E. P., & Özcan, T. 2019, s.3)

1.5. Dolandırıcılıktan Korunma Yöntemleri

Dolandırıcılık ile mücadelede alınması gereken önlemlerde hem kişilere hem de kurumlara ciddi görevler düşmektedir. Zamanla dolandırıcılar kendilerini geliştirdikçe dolandırıcılara karşı alınması gereken önlemler de gelişecektir. Günümüzde müşteriler ve bankalarca dolandırıcılıkla mücadele konusunda alınabilecek önlemlere aşağıda yer verilmiştir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

1.5.1 Bankalar Tarafından Kullanılan Güvenlik Unsurları

Bankalarca kullanılan güvenlik önlemleri müşterilerinin finansal değerlerini ve işlem güvenliklerini korumaya yöneliktir. Bunun için bankalarca sunulan mobil bankacılı, internet bankacılığı, ATM, telefon bankacılığı gibi alternatif dağıtım kanalları ve uzaktan müşteri olma uygulamaları için tasarlanmış maksimum güvenlik önlemlerinin alındığı ortamlardır. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

***Müşteri Numarası/Kullanıcı Adı:** Bankalarca müşterisine özel tanımlanan firmaya veya kişiye özel bir kodlamadır.

***Şifre/Parola:** Kimlik doğrulama için kullanılmakta olan, belirli zamanlarda değiştirilmesi gerekli olan gizli rakam ve/veya harf içeren karakterler serisidir.

***OTP/SMS:** Dijital haberleşme işletmecileri tarafından sunulan kısa mesaj(SMS) servisiyle iletilen tek kullanımlık şifrelerdir.

***Tek Kullanımlık Şifre/Parola:** Kimlik doğrulama için yalnız bir defa kullanılmak üzere rastgele oluşturulmuş rakam ve harflerden oluşan karakterler dizisidir.

***Hassas Veri:** Kimlik doğrulama için kullanılmakta olan veriler öncelikli olmakla beraber; müşterilere ait olan, çeşitli nedenlerle banka tarafından saklanan ve 3. şahıslarca ele geçirilmesi durumunda, bu şahısların gerçek müşterilerle ayırt edilebilme mekanizmasının zarar göreceği ve dolandırıcılık veya müşteri adına sahte işlem yapılmasına imkân tanıyabilecek nitelikli verilerdir.

***Güvenlik Resmi:** Bankalarca internet ve mobil bankacılığa girişte gösterilmekte olan ve daha önce müşterilerce seçilen kod/resimdir. Bu sayede müşteri tarafından giriş yapılan sitenin müşterinin çalıştığı bankaya ait olduğu teyit edilir.

***Elektronik İmza(E-İmza):** 15.01.2004 tarihli ve 5070 sayılı Elektronik İmza Kanununda tanımlanmış kişilere özel elektronik imza sertifikasıdır.

***Müşteri Bilgilendirmeleri:** Bankaların SMS/e-mail yoluyla ya da internet sitelerinde müşterilere güvenlik ile alakalı yaptıkları bildirimlerdir.

***Mobil Cihaz Onayı:** Aktifleştirilen mobil cihaz üzerinden alınmakta olan onaydır.

***Biyometrik Kimlik Doğrulama:** Kimlik doğrulama işleminin gerçekleştirilmesi maksadıyla kullanılmakta olan kişilere özgü ölçülebilir davranışsal veya biyolojik karakteristiktir.

***Yakın Alan İletişimi (NFC):** Elektronik cihazların temassız, güvenli işlem yapabilmesini ve sayısal içeriğe ve/veya elektronik cihazlara erişimini sağlayan, veri okuma ve yazmada kullanılan kısa menzilli kablosuz teknolojidir.

1.5.2 Müşteriler Tarafından Alınması Gereken Önlemler

Bankalarca alınan güvenlik tedbirleri tek başına yeterli gelmemektedir. Alınan bu tedbirlere ek müşterilerin de öncelikli olarak alması gerek bazı önlemler ve uyması gereken bazı kurallar vardır.

***Bildirimlerle Gelen Linkler:** Kaynağı belli olmayan ya da emin olmadığınız SMS(kısa mesaj), anlık haberleşme uygulamalarından gelen mesajlar, sosyal medya reklamları ve e-mail gönderilerinin içerisindeki linklere tıklamayın ve bu gönderileri açmayınız.

*__Mobil Uygulamalar:__ Yaygın ve bilinen uygulamalar dışında, güvenliğinden emin olmadığınız uygulamaları kesinlikle yüklemeyin ve bu uygulamaları açmayınız. Resmi olmayan uygulama mağazalarındaki ortamlardan kesinlikle uygulamalar indirmeyiniz.

***Kimlik Bilgilerinin Gizliliği:** Banka işlemlerinde kullanılmakta olan kimliklerin güvenliği oldukça önem arz ettiği için, kimliklerin taranan görselleri bilgisayarda saklanmamalı, fotokopileri her yerde bulundurulmamalıdır.

***Kart Bilgilerinin Güvenliği:** Kartta bulunan bilgiler kişilere özeldir ve bu bilgilerin gizliliğini (son kullanma tarihi, kart numarası, CVV2/güvenlik kodu) koruyunuz. Güvenliğinden endişe duyduğunuz ve emin olunmayan uygulamalar, web sitelerinde kullanmayınız, 3.şahıslarla paylaşmayınız. Kart ile sanal ortamda yapılan alışverişlerinizde sanal kart tercih ediniz.

***Parola/Şifre Bilgilerinin Gizliliği:** Bankacılık işlemlerinde kullanılan parola/şifre (tek kullanımlık şifre, kart şifresi) kişilere özeldir ve gizliliğinin/güvenliğinin sağlanması müşterilerin sorumluluğundadır. Parola/Şifre bilgilerinin tahmini kolay olmayacak şekilde (doğum yılı vb.) oluşturulması büyük önem arz etmektedir.

Kamuya açık (ortak kullanıma) tahsis edilen ve güvenliğinden emin olmadığınız cihazlardan bankacılık kanallarına giriş yapmayınız. Ayrıca kamuya (ortak kullanıma) açık kablosuz bağlantılar üzerinden bankacılık işlemlerini yapmayınız. POS ve ATM gibi ortak kullanıma açık alanlarda yapılacak bankacılık işlemlerinde kullandığınız parolaların, üçüncü kişiler tarafından görülmeyecek şekilde girişlerinin yapılması büyük önem arz etmektedir.

***Bankalardan Gelen Bildirimler:** Bankacılık ürünlerinin güvenliği ile alakalı konular hakkında bankalarca verilen açıklamaların/bilgilerin okunması ve belirtilen talimatlara uygun olarak hareket edilmesi güvenlik açısından son derece önemlidir.

Güvenlikle alakalı en ufak bir şüphe ve tereddüt oluşması halinde mutlaka bankaya başvurularak ve banka bilgilendirilmelidir. Unutmayınız, bankalar kişisel verileri müşterilerden asla e-mail yoluyla istemezler.

Kişisel verileri talep eden e-mail ve/veya e-mail içinde bulunan linkler üzerinden bilgi paylaşımı yapılmamalı, cevap gönderilmemeli ve bu gibi durumlarla karşılaşıldığında derhal bankalara bilgi verilmelidir.

Bankalar tarafından yayınlanan güvenlik duyuruları sürekli takip edilmeli ve bu duyurularla gönderilen uyarılara dikkat edilmelidir.

***Bankacılık İşlemi Yapılan Cihazın Güvenliği:** Bankacılık işlemlerinin yapıldığı cihazların işletim sistemleri ve internet tarayıcıları güncel tutulmalıdır. Bu cihazlarda lisanslı ‘’anti-virüs’’ yazılımları kullanılmalıdır ve bu yazılımlar periyodik olarak güncellenmelidir. Bankacılık işlemlerinde kullanılan cep telefonları da dahil olmak üzere bütün cihazların güvenliği müşterilerin sorumluluğunda olup, bu cihazların üçüncü kişilerce kullanılmasına izin verilmemelidir.

***İletişim Bilgilerinin Güncelliği:** Bankaların müşterileri adına yapılan işlemlerle ilgili bilgilendirmeler yaptığı ve şüpheli işlem bildirimlerinde ulaşmak amacıyla kullanılan iletişim adreslerinin (e-mail bilgisi, cep telefonu numarası, iş/ev adresi vb.) banka kayıtlarında sürekli güncel tutulması büyük önem arz etmektedir. Bu adreslerde yapılacak değişiklikler müşteriler tarafından bankalara zamanında bildirilmelidir.

1.5.3 Bilgi Güvenliği/Veri sızıntısı

Bilgi güvenliği, bir varlık olarak bilginin yetkisiz ve izinsiz kullanımının, 3.şahıslarca ele geçirilmesi, değiştirilmesi, yok edilmesi ve bilgilere hasar verilmesinin önlenmesi amacıyla kurumlar nezdinde alınan önlemler, bu amaçlarla işletilen politikalar ve kurulan sistemler olarak ifade edilmektedir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

Veri sızıntısı, müşteri ve kurumlara ait bilgilerin bilinçli ya da bilinçsiz şekilde izin alınmaksızın kurum dışına çıkarılarak belirlenen bilgi güvenliği politikalarının ihlalidir.

1.5.3.A- Veri Sızıntısına Sebep Olan Yöntemler

Kurumlarda bilgiler sunucu, diz üstü ve kişisel bilgisayarlar, akıllı telefonlar, tabletler, veri tabanı, taşınabilir diskler, elektronik posta, DVD ROM/CD, kâğıt gibi ortamlarda yer alabilmektedir. Bu sebeple veri sızıntısı vakalarında, bu ortamlara yönelik atak yapılmakta ve ele geçirilen veriler hızlı şekilde kurum dışına çıkarılmaya çalışılmaktadır. Veri sızıntısına yol açan ihlaller aşağıdaki yöntemlerle gerçekleşebilmektedir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

***Giden Elektronik posta:** Elektronik posta iletileri, banka sistemindeki her türlü veri ve bilgiyi sızdırmak için kullanılabilir. Bu bilgiler ve veriler, bir e-mail ya da metin mesajı veya bir dosya eki olarak 3.şahıslara aktarılabilir.

***Güvenli Olmayan Cihazlara İndirilen Dosyalar:** Kurumlarca kullanıcısına tahsis edilmeyen cihazlar(kişisel kullanımda olan bilgisayar, cep telefonu, usb bellek, tablet, kamera, DVD/CD-ROM vb.) ile herhangi bir kurum veri ve bilgisinin kopyalanması, indirilmesi, suretiyle bilgiler kurum dışına çıkartılabilir. Güvenli olmayışı ve kurum tarafından izlenememesi sebebiyle verilerin bu cihazlarda saklanması oldukça risklidir.

***Fiziki Belgeler ve Çıktılar:** Fiziki belgeler üzerinde bulunan veriler/belgeler ve elektronik ortamlardan alınan fiziki çıktı ve belgeler en az elektronik ortamlarda saklanan veriler kadar önemlidir. Bu ortamlarda bulunan verilerin takibi ve kontrolü oldukça zor olduğundan veri sızıntısında kullanılmakta olan önemli yöntemlerdir. Ayrıca, şahısların ve şirket/firmaların değersiz olarak gördükleri, üzerinde bilgiler bulunan her türlü materyallerin çöp kutularına atılabildiği ve bu atıkların art niyetli şahıslar tarafından bilgilere ulaşmak amacıyla toplandıkları görülmüştür. Bir çöp kutusundaki atıklarda, kurumun iş yaptığı şahıslara ait ünvanları, telefon bilgileri, organizasyon şemaları ve çalışanlarının adı, soyadı, günü geçmiş DVD, CD, toplantı konu ve tarihleri, dekontlar, hesap hareketleri gibi kaynaklar bulunabilmektedir.

1.5.3.B- Veri Sızıntısından Korunma Yöntemleri

Bilgi güvenliği prensiplerinin uygulanmasından kurum kadar kurumda çalışan personelin de sorumluluğu bulunmaktadır. Kurum, veri sızıntılarına engel olmak adına gereken teknik ve fiziki altyapıyı oluşturmalıdır ve bu sistemleri belirli periyotlarda düzenli şekilde güncellemesi gerekmektedir. Kurum çalışanlarıysa, gerek kurumca personele tahsis edilmiş cihazların güvenliklerini sağlamakla ve uygulamalarda kullandığı kimlik doğrulama unsurlarını korumakla görevlidir. Veri sızıntılarına engel olmak için dikkat edilmesi gereken hususlar aşağıda belirtilmiştir. (URL1: https://www.tbb.org.tr/tr (Erişim Tarihi: 05.01.2022)

1.5.3.B.1 – Parola Güvenliği

***Farklı Şifre/Parola:** Kullandığınız tüm hesaplarınız için farklı şifre kullanın; kurumda

Kullanılan şifreleri başka yerlerde kullanmayın.

***Kamuya Açık Bilgisayarlar:** Güvenliğinden endişe duyduğunuz, emin olmadığınız veya kontrolü sizde bulunmayan ortak kullanıma açık bilgisayarlarda veya ağlarda şifrelerinizi kullanmayınız.

***İki Aşamalı Doğrulama:** Kullandığınız tüm hesaplarda 2 aşamalı kimlik doğrulama kullanın.

***Şifre/Parola Gizliliği:** Şifrelerinizi kesinlikle başkalarıyla paylaşmayın.

***Parola/Şifre Değişikliği:** Kimlik bilgilerinizi ve size ait olan bilgilerinizi şifrelerinizde kullanmayın, şifrelerinizi belirli periyotlarda değiştirin.

***Güçlü Şifre/Parola:** Şifrelerinizi, karışık rakam ve karakterler kullanıp tahmini zor bir şekilde belirleyin.

1.5.3.B.2 – Cihaz Güvenliği

***Güncelleme:** Kurumuzca size tahsis edilen cihazların güvenlik ayarlarıyla oynamayın, güncellemelerinizi zamanı geldiğinde yapın.

***İşyerinde Kişisel Donanım:** Kuruma ait cihazlara kişisel aygıt bağlamayın, iş dışındaki bir amaç için kullanmayın.

***Alarm Durumu:** Cihazlarınızda anormal bir durumla karşılaştığınızda (anti-virüs uygulamasının alert üretmesi, uygulamaların/ekranın kendiliğinden açılıp kapanması vb.) hiçbir işlem yapmadan en hızlı şekilde teknik birimlere haber verin.

1.5.3.B.3 – E-Posta Güvenliği

***Kurum E-postaları:** Kurumlarca çalışanlara tahsis edilmiş e-mail adreslerini işiniz dışındaki başka amaçlarla kullanmayınız.

***Kişisel E-postalar:** Kişisel e-postalarınızı iş amacıyla kullanmayınız.

***Hassas Bilgi Paylaşımları:** Hassas ve gizli veri sınıflarında bulunan bilgileri e-mail ile kurum dışına göndermeyiniz.

***Abonelik İstekleri:** İş dışındaki web sayfalarına üye olunurken kuruma ait e-mail adreslerini kullanmayınız.

***Şifre/Parola Gizliliği:** Parola/Şifre bilgilerinizi e-mail ortamlarında paylaşmayınız.

***Şüpheli E-posta:** Kaynaklarından emin olmadığınız ve şüphe duyulan, şüpheli e-mail gönderilerini açmayınız, içinde bulunan linklere tıklamayınız.

1.5.3.B.4 – Genel Güvenlik İpuçları

***Modem Güncelleme:** Evde kullanılan modemlerinizi sürekli en son sürümünde kullanın.

***Modem Şifresi:** Kullandığınız modemin kullanıcı adı/şifre bilgilerini değiştirin ve yazılımları sürekli güncelleyin.

***Cihaz Güncellemeleri:** Tablet, bilgisayar, telefon gibi cihazlarınızın sürekli sürüm güncellemelerini yapın.

***Güçlü Şifre/Parola:** Kolay şifreler kullanmayın, kesinlikle ikili doğrulama ayarlarınızı yapın.

***Güvensiz Linkler:** Güvenliğinden şüphe duyduğunuz, emin olmadığınız kaynaklardan iletilen linklere tıklamayın.

***Web Adresi Doğruluğu:** Girmeyi düşündüğünüz web sayfasının adreslerinin doğruluğunu teyit edin.

***Kurum İçi Eğilimler:** Kurumunuza ait bilgi güvenlikleri ile alakalı paylaşımları dikkatlice takip edin ve eğitimlerinizi belirlenen zamanda tamamlayın.

SONUÇ

Dolandırıcılık yapmak isteyen dolandırıcılar, kişi veya cinsiyet ayrımı asla yapmazlar. Çeşitli endüstrilerde ve coğrafi konumlarda büyük veya küçük şirketlerde her türlü dolandırıcılık faaliyeti olabilir. Çalışan sahtekarlığı, sonuçta bir organizasyonun çöküşüne yol açabilecek büyük mali kayıplara, yasal maliyetlere ve mahvolmuş itibarlara neden olabilir. Uygun planların yürürlükte olması, dolandırıcılık faaliyetlerinin oluşmasını önemli ölçüde azaltabilir veya halihazırda bir dolandırıcılık gerçekleşmişse kayıpları azaltabilir. Şirket politikasını çalışanlara bildirmek, hileli davranışları caydırmanın en iyi yollarından biridir.

Politikayı takip etmek ve biri yakalandığında belirtilen adımları ve sonuçları uygulamak, dolandırıcılığı önlemek için oldukça önem arz etmektedir. Bir işletme için sahtekarlığı önlemeye çalışmanın maliyeti de işlenen sahtekarlığın maliyetinden çok daha ucuz olduğu görülmektedir.

Dolandırıcılık amacıyla kurulmuş çetelerin ve dolandırıcıların hedefinde şahıslarla beraber kurumlar da bulunmaktadır. Son dönemlerde de Türkiye'de ve Dünya'da bankacılığın Alternatif Dağıtım Kanallarının (dijital kanallarının) kullanım durumunun artış göstermesi ve bireylerin eski dönemlerde yastık altlarında tutmuş oldukları birikimlerini bankalara yatırması sonucunda, bankalar ile çalışan müşteri sayılarında ve kullanılan ürünlerde ciddi artışlar meydana gelmiştir. Banka kullanımının artması ve doğası gereği parayı barındıran bu kurumlar, art niyetli dolandırıcıların iştahını kabartarak bankalar ve müşterileri üzerine yoğunlaşmalarına sebep olmuştur.

Bankacılık sektörü, dolandırıcılık eylemlerine en çok hedef olan sektörlerin başında gelmektedir. Bu sebeple bankaların, teknolojik altyapıların kurulması ve bankacılık işlemlerinin gerçekleştirilmesi konularında basiretli hareket etmeleri büyük önem taşımaktadır.

Gelişen teknolojiler ile dijital kanallar her geçen gün hayatımızın bir parçası haline gelmektedir. Bankacılık sektörü de gelişen teknolojilere ayak uydurmakta ve dijitalleşme adına sistemlerini sürekli geliştirmektedir. Gelişen teknolojiler ve dijitalleşme hayatı her ne kadar kolaylaştırsa da oluşabilecek riskleri de beraberinde getirmektedir. Hazırlanan bu çalışmada dijitalleşme ile beraber olası dolandırıcılık girişimlerinden bahsedilmiş ve alınması gereken önlemlere kısaca değinilmiştir.

Bankacılık sektöründe yaşanan Dolandırıcılık eylemleri hem bankalar için hem de banka müşterileri için ciddi sonuçlar doğurmaktadır. Müşteriler açısından maddi kayıplara neden olan dolandırıcılık eylemleri Bankalar açısından da maddi kayıplar dışında itibar kaybına da sebep olmaktadır. Bu kapsamda bankalar bilgi teknolojileri ve güvenlik ağlarını sürekli güncel tutmalı, gerekli tedbirleri alarak müşterilerini sürekli bilgilendirmelidirler. Müşteriler ise bankaların güvenlik bildirimlerini sürekli takip etmeli ve bankaların belirlediği tedbirleri almalıdırlar.

KAYNAKÇA

Aktaş, M. M. (2019). Borsa İstanbul AŞ piyasalarında uygulanacak gözetim tedbirleri yönergesi'nin işlem bazlı piyasa dolandırıcılığı suçu bakımından değerlendirilmesi. Uyuşmazlık Mahkemesi Dergisi, 7(14), 1-23

Bahar, A. (2020). İkna Yoluyla Dolandırıcılık: Dolandırıcılık Faaliyetlerinde İkna ve Etkili İletişim Yöntemlerinin Tespiti Üzerine Bir Araştırma. Türkiye İletişim Araştırmaları Dergisi, (35), 139-163.

Çakır, H., & Yaşar, H. (2015). Kurumsal Siber Güvenliğe Yönelik Tehditler ve Önlemleri. Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 3(2), 488-507.

Çolaklar, Gültekin, Şeşen, N. (2023). An Overview of the Curricula of Medical Documentation and Secretarial Programs Using the Distance Learning Method in Turkey. Journal of Balkan Libraries Union 10(1), 1-12

Erdoğan, M. (2021). İşletmelerin Kâbusu: İş E-Postası Dolandırıcılığı (BEC). İşletme Akademisi Dergisi, 2(2), 208-219.

Kolukırık, S., & Gün, E. (2020). Bilişim Teknolojilerinin Suç Eylemi Üzerindeki Etkisi: İnternet Haberlerinde Dijital Suç Örneği. Journal of World of Turks/Zeitschrift für die Welt der Türken, 12(3), 8-10.

Maviş, V. (2015). Dolandırıcılık suçunun hile unsuruna ilişkin sorunlar. İnönü Üniversitesi Hukuk Fakültesi Dergisi, 6(3), 597-626.

Özcan, N.(2012). Dolandırıcılık Suçu. Çankaya Üniversitesi Sosyal Bilimler Enstitüsü. Yayımlanmamış Yüksek Lisans Tezi. Ankara.

Özmen, E. P., & Özcan, T. (2019). Dolandırıcılık tespiti üzerine melez sınıflandırma ve regresyon ağacı uygulaması. Yönetim Bilişim Sistemleri Dergisi, 5(2), 12-20.

Şenol, A. ve Karacan, H. (2012). "Savan Avlama (Phishing): Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri". 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, https://www.researchgate.net/profile/Ali_Senol/publication/269405477_Sazan_Avlama_Phishing_Kullanilan_Teknikler_ve_Bunlardan_Korunma_Yontemleri/links/5d908491299bf10cff1888e7/Sazan-Avlama-Phishing-Kullanilan-Teknikler-ve-Bunlardan-KorunmaYoentemleri.pdf , Erişim Tarihi:10.12.2020

Türkiye Bankalar Birliği (2022) , Dolandırıcılık Eylemleri ve Korunma Yöntemleri- Bankacılar Nüshası Kitabı (TBB 2022)

Yelken, C. (2019). Bankacılıkta dolandırıcılık eylemleri ve önlenmesine yönelik yöntemler: banka uygulaması. (Yüksek Lisans Tezi). Marmara Üniversitesi, İstanbul (Turkey).